Quality Assurance Plan

D7.2

Project reference no. 653884

December 2015

European Commission

Horizon 2020
European Union funding
for Research & Innovation

Document information

Scheduled delivery	16.01.2017
Actual delivery	16.01.2017
Version	2.1
Responsible Partner	INESC TEC

Dissemination level

Public

Revision history

Date	Editor	Status	Version	Changes
05.11.2015	R. Oliveira	Draft	0.1	ToC
20.11.2015	R. Oliveira	Draft	0.2	Complete Draft
24.11.2015	R. Oliveira	Draft	0.3	Revised complete draft
20.12.2015	H. Mercier	Draft	0.4	Revised complete draft
20.12.2015	R. Oliveira	Submission	1.0	
12.01.2017	F. Maia	Revision	2.0	Incorporated feedback from 1st year review.
14.01.2017	R. Oliveira	Revision	2.1	Revised final version

Contributors

F. Maia (INESC TEC)
J. Paulo (INESC TEC)
R. Oliveira (INESC TEC)

Internal reviewers

M. Barbosa (INESC TEC)
H. Mercier (UniNE)

Acknowledgements

This project is partially funded by the European Commission Horizon 2020 work programme under grant agreement no. 653884.

More information

Additional information and public deliverables of SafeCloud can be found at http://www.safecloud-project.eu

Glossary of acronyms

Acronym	Definition
D	Deliverable
DoA	Description of Work
EC	European Commission
PM	Project Manager
PO	Project Officer
WP	Work Package

Table of contents

1 Executive summary

The Quality Assurance Plan establishes the foundation for the SafeCloud project structures and supporting processes. All the SafeCloud partners should follow it in order to ensure the quality of the work performed within the project.

The management structure and decision-taking mechanisms will support the consortium in its day-to-day activities. The communication mechanisms are essential, as decisions are made according to the available information at a certain moment. The verification of project deliverables is also a major part of the quality assurance.

All partners are involved in the quality assurance activities, on grounds of their different roles and responsibilities.

2 Introduction

2.1 Purpose of the document

This document presents the Quality Assurance Plan for the Horizon 2020 project SafeCloud. The objectives of this Quality Assurance Plan are:

- To lay out a common practice among project partners about quality procedures.
- To assist each individual development team in implementing decisions in their environment.
- To provide measurement criteria to verify the quality of the project.
- To provide each partner and the European Commission (EC) with sufficient visibility about the consortium and its quality practices.

This quality plan describes the project quality assurance approach, as well as the procedures and tools that the consortium has to follow for partner communication, documentation, deliverable production, review, and reporting.

2.2 Quality of glossary terminology

This glossary presents the terms used in the quality standards [Int14] and is further on exploited within this document:

Quality: The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs.

Quality Assurance (QA): All those planned and systematic actions necessary to provide adequate confidence that a product or service will satisfy given quality requirements. The QA evaluates the performance of the project and produces recommended actions and change requests.

Quality Record: Written records that are retained.

Quality Control: The operational techniques and activities that are used to fulfil requirements for quality.

Quality Management System: The management system to direct and control an organisation with respect to Quality. This system is made of interacting or interrelating elements, such as structures, responsibilities, procedures, processes and resources, for implementing the quality.

Project Quality Plan: Set of activities planned at the beginning of the project that helps achieve Quality in the Project being executed.

Verification: Reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether items, processes, services, or documents conform to specified requirements.

2.3 Structure of the document

The quality assurance plan is organised as follows. In Section 2, we present an overview of how quality will be managed and ensured through the corresponding processes in the consortium. We consider a wide set of processes from meetings to reporting procedures. We also describe a risk management procedure that facilitates the identification, analysis and mitigation of potential risky situations. All partners are involved in the risk management activities, according to different roles and responsibilities. In Section 3, we introduce the collaborative tools, formats and templates that will be used within the consortium.

3 Quality management

This section looks at the main processes deployed in the project and highlights the procedures to comply with quality standards.

3.1 Project monitoring and quality control

Project monitoring is a crucial procedure whose objective is to keep a mindful control of activities during the project. According to the Description of Action (DoA), the project execution is supervised by the Project Management Board (PMB) which is the core organisational and decision-making body, reporting back to the Executive Board for key-decisions that affect the structure and success of the project.

This monitoring process will be based on the internal WP reports, generated midway through each reporting period. These reports will inform about the progress at WP level towards the objectives, progress, status and next steps. Each Work Package Leader (WPL) will prepare a report on her / his WP (other contributors to the WP will assist the WPL with the reporting) and submit it to the Project Coordinator (PC). The PC and the Scientific & Technical Director (STD) will integrate and review all contributions in a full document. At the same time, each partner will produce a report explaining their participation in the project work along the six-month period and the use of his resources. These reports will aim at the regulation of the project funds, according to the payment procedure established in the Consortium Agreement (CA).

Quality is also a part of this project monitoring. The establishment of certain procedures at the beginning of the project does not imply they are sacrosanct. It is important to check the effectiveness of these procedures (the Quality Assurance Plan itself) and modify them as needed to counter any weaknesses or deficiencies in the project execution.

3.2 Contractual processes

3.2.1 Amendments to the Grant Agreement

Should the grant agreement need to be changed, any request for amendment (i.e. addition, removal or modification of special clauses, modification of reporting periods) shall be submitted in accordance with the procedures and provisions within the "Annotated Model Grant Agreement" [Eur15].

3.2.2 Changes in the Consortium

Joint of new partners
If required by the project development needs, the consortium may propose to the EC the participation of a new partner, in conformity with the stipulations of "Annotated Model Grant Agreement" [Eur15]. This new partner shall be proposed by project's partners and approved by the Executive Board (EB).

Withdrawal of partners
The consortium may communicate to the EC the withdrawal of a partner, in conformity with the stipulations of "Annotated Model Grant Agreement" [Eur15]. The withdrawal of a partner may be requested by the partner itself to the coordinator, or by the consortium, according to the provisions of the CA.

3.3 Communication processes

3.3.1 Communication

Constant and effective communication among all project stakeholders is necessary to ensure the success of any project. There are two directions for the information flow:

Internal communication
Internal communication refers to communication among the consortium partners aiming at the development of project technologies. From a quality perspective, communication must be reliable and effective but also economical. Therefore this will happen mainly through email exchanges, teleconferences and meetings (in order of likelihood).

The STD is responsible for providing and maintaining the internal communication tools at a high level. This role can be also taken by other roles at WP level.

External communication
External communication refers to communication with external stakeholders, such as related initiatives, R&D projects, target users, Project Officer (PO), and other representatives of the EC. External stakeholders must be kept informed about the progress and results of the project. The management of their expectations is also key in order to create impact. In this sense, dissemination activities and tools are the most suitable channel for information flow.

The coordinator is responsible for managing the Project communication with external initiatives. Nevertheless, any partner is in principle entitled to take dissemination actions, although there should be a coordinated action under the dissemination and communication task leader. Likewise, external stakeholders can play an important role in the project by providing inputs ranking from technical support to advice that can help to tune the project with the existing communities and avoid any work duplication. The clustering initiatives and the workshops seem to be the best manner to channel this kind of information.

3.3.2 Project meetings

Face-to-face meetings and teleconferences are needed to tackle discussions on important matters that require the participation and opinion of all partners. They also represent a central quality and risk management tool in order to identify problems, define actions, propose contingency plans, and agree on decisions.

Meeting roles
It is worth distinguishing among these main roles:

- The chairperson: determines the meeting objectives and plans, and is responsible for the overall direction of the meeting.
- The facilitator: hosts the teleconference or deals with local organization of the on-site meeting.
- The recorder: keeps track of the vital information from the meeting. In principle, the chairperson and the recorder will be the same.
- The participants: a group of individuals responsible for getting the job done, generate ideas, analyse information, make decisions, and implement action plans.

Management meetings
Management meetings are mainly those of the Executive Board (EB) and the Project Management Board (PMB):

- **EB meetings:**
  - The EB will gather regularly, at least twice a year.
  - The PC will be the chairperson of the meeting and be responsible for the agenda and the minutes.
  - Each time the meeting will be organised by a different partner of the Executive Board (the facilitator).
  - When feasible, EB meetings will be organized in conjunction with other major events (e.g. the two project workshops) to minimize travel costs.
  - Extraordinary meetings can be held at any time upon request of the project coordinator, the Project Management Board (PMB) or one-third (1/3) of the members of the EB.
- **PMB meetings:**
  - Meetings will be convened by the PC, though it would be advisable to have at least one meeting every month.
  - They are expected to be teleconferences.
  - The PC will be the chairperson of the meeting and will be responsible for the agenda and the minutes.
  - Extraordinary meetings can be held at any time upon request of any member of the PMB.

Technical meetings
These refer to the Scientific & Technical Committee (STC) or Work Packages.

- **STC meetings:**
  - The STC will gather every month by teleconference.
  - The STD will be the chairperson of the meeting.
  - When feasible, STC face-to-face meetings will be organized in conjunction with other events (e.g: the EB meetings) to minimize travel costs.
  - Extraordinary meetings can be held at any time upon request of any member of the PMC.
- **WP meetings:**
  - Meetings will be convened by the Work Package Leader, though it would be advisable to have one teleconference at least every 2 months.
  - Though they are expected to be teleconferences, face-to-face meetings could be possible.
  - The WPL will be the chairperson of the meeting and will be responsible for the agenda and the minutes.
  - Extraordinary meetings can be held at any time upon request of any member of the respective WP.

Meeting agenda
All meetings will have an agenda. The agenda will comprise a list of the expected attendees (audience), topics to be discussed (with timetable), supporting or required material (if any), and venue address (only for onsite meetings).

The chairperson will prepare the agenda in cooperation with the meeting facilitator.

The agenda should be distributed long enough ahead of time so that any necessary preparation by the participants can be completed.

Meetings recording
After the meeting the chairperson will generate the meeting minutes to have a written proof of it. This aims at two main purposes: firstly, minutes are another communication mean for those absent partners, so that they can be informed about the contents of the meeting, decisions taken and action points (deadline and responsible); secondly, minutes help tracking meetings and course of events.

Recording of details should be kept to a minimum. Chronological order need not be respected unless it is critical for understanding. Circulation of the minutes must be done within one (1) week after the meeting. All partners have the right to provide comments to the text. The chairperson will store a copy of the minute's document in the project repository under the corresponding meeting folder.

Participation in meetings
Each participant to a meeting should contribute to its preparation by providing in advance to the meeting:

- Working documents and presentations for the meeting. As far as possible, these papers should be available at the project repository in advance (seven days (7) before) and not during the meeting itself, since otherwise the participants will be unable to prepare for the meeting.
- Contributions to the agenda.
- Feedback on the subsequent minutes.
- Executions of actions and respect of decisions.
- In case of on-site meetings, information related to meeting venue, arrival and accommodation (this only applies to the facilitator).
- For teleconferences, connection details and indications on how to participate (this only applies to the facilitator).

3.4 Reporting process

Reporting is one of the most important communication channels between the consortium and the EC. This communication consists of specific reports produced at different times regulated by the Grant Agreement (GA). The general responsibility of the reporting process belongs to the PC, though all partners assist her / him in this task. The PC forwards the reports to the PO.

3.4.1 Periodic report

In the DoA there are two reporting periods as stated in the GA

- Period 1 (M12): from Month 1 (September 2015) to Month 12 (August 2016).
- Period 2 (M36): from Month 13 (September 2016) to Month 36 (August 2018).

As indicated in the Annex II of the GA, the consortium shall submit a periodic report to the Commission for each reporting period within sixty (60) days after the end of each respective period. This reporting period is an accurate description of the work carried out in the project for each phase, as well as an explanation of the use of the resources. The periodic reports will also include a scientific reporting part that will provide overview of the objectives for the period, the work progress and achievements during the period, as well as deliverables and milestones information.

3.4.2 Final reporting

At the end of the project, a Final Report should be submitted within 60 days after the end of the project. The Final Report will, acording to Article 20.4, include a final technical report with a summary for publication containing: (i) an overview of the results and their exploitation and dissemination; (ii) the conclusions on the action, and (iii) the socio-economic impact of the action, and a final financial report containing: (i) a 'final summary financial statement', created automatically by the electronic exchange system, consolidating the individual financial statements for all reporting periods and including the request for payment of the balance and (ii) a 'certificate on the financial statements' for each beneficiary , if it requests a total contribution of EUR 325 000 or more, as reimbursement of actual costs and unit costs calculated on the basis of its usual cost accounting practices.

3.5 Deliverables process

Deliverables are the official and contractual documents between the Consortium and the EC. Therefore deliverables must follow a conveyance process in order to assure their consistency and their quality.

A bottom-up strategy is chosen for quality control. This implicates a continuous and gradual process at every phase, starting from the very first stages until the final delivery, in which all partners are involved. The delivery process is as follows.

- The deliverable relates to a specific WP. The responsibility of the document lies on the lead beneficiary, as indicated in the list of deliverables of the contractual document (DoA). She/He is the main author and the deliverable editor.
- All partners working in this WP are the deliverable contributors. They are expected to contribute to the production of the deliverable and review of partial versions.
- Delivery dates are defined in the DoA.
- Upon decision of the main author, the deliverable is submitted to a review process at least two weeks ahead of due date. Reviews are control mechanisms for quality control and assurance.
- Two reviewers will be involved in the internal review. The review will be performed by the WP leader and another individual appointed by the editor (preferably from a different partner to the WP leader and the editor).

The deliverable editor will agree with the proposed person his role as reviewer. If conflict arises or no reviewers can be found, the deliverable editor can contact the project Coordinator to identify potential reviewers.

- Both reviewers will check issues such as:
  - Coverage of all relevant aspects and coherence of ideas.
  - Readability of the text.
  - Adequate explanations of terms.
  - Appropriate level of detail.
  - Use of references and acronyms.
  - Compliance with the official template.
  - Appearance.
  - Other aspects.

The reviewers have one (1) week to provide comments to the author. These comments are sent to the author through a Document Review Sheet (DRS) or inline as part of the working document. The use of Word documents with track changes is chosen whenever possible.

- The review is registered in the version history of the document. The reviewer's names are also visible on the cover page.
- The result of the review is stored at the project repository for the record (Quality reports).
- The author answers to the comments and generates the final version of the deliverable.
- In the case of official deliverables, the author shall submit that final version of the deliverable to the Project Coordinator for approval at least two (2) days before the due date. In the case of large deliverables, it is highly advisable that the WP leader requests intermediate versions, which will be reviewed following the same process as for the final version, except for the Project Coordinator check which is done only for the final version.
- For official deliverables, the Project Coordinator sends the deliverable to the Project Officer (PO) in PDF format, as representative of the European Commission.
- The evaluation of the deliverable will take place at the end of each reporting period, according to the clauses of the GA.

3.6 Software deliverables

Some of the SafeCloud deliverables are software prototypes (demonstrators) that require specific quality control mechanisms. Their development is based on an agile methodology. The implementation is performed incrementally producing a series of versions. In order to provide the snapshots of the work plan, two major versions will be produced for every piece of delivered software. A first version with a preliminary working implementation. And then, a second version with the final implementation. These two versions will also serve as major milestones in the project for the different components (M2), integrated platform (M3) and deployment (M4).
The development methodology will be accompanied with an agile management tool ecosystem including a global documentation, a ticket system, software versioned repository, and a project building system.

These deliverables will follow the quality guidelines discussed in Section 3.5 plus the following quality process.

- Three different types of tests will be devised to ensure that solutions being developed comply with the desired performance, functionality, and APIs.
  - Unit testing – small and contained tests will be devised for evaluating small components of solutions being devised in each WP.
  - Independent WP integration testing – higher-level and more complex tests will be devised to comprehensively evaluate each individual solution provided in each WP.
  - Cross WP integration testing – Since some of the use-cases require the integration of solutions from different WPs, integration tests must also be built to evaluate integrated solutions. These tests will be complemented with use case workloads to verify that each solution satisfies their requirements appropriately.
- Continuous testing – all the previous tests will be available to all the partners involved in the corresponding solution so that every time the implementation of a software component evolves, there is a battery of tests that can be performed to check if the newer implementation still complies with the desired performance, functionality, and APIs.

- Cross-partner testing – Each partner using a software component provided by another SafeCloud consortium member will test such component in their own environment. This will allow to further validate if each component offers the required functional and non-functional characteristics.

3.7 Document deliverables

3.7.1 Documents language

English is the official language of the project. All relevant documents must be written in English. Nevertheless there can be exceptions with regard to dissemination materials, such as press releases that can be translated to other languages (mainly the consortium languages) or technical publications.

3.7.2 Documents naming

Each document identified with a unique code, regardless of the filenames and referencing conventions that each partner is free to use in local archives. The aim of these codes is to give clear access to the project documentation, for internal purposes.

Official deliverables

Regarding the deliverables, the code is defined as follows:

SafeCloud-Dx.y-Deliverable Name-vn.m

Where:

- Dx.y is the deliverable number, as reported in the cover page of the document. The resulting identifier must be one of that listed in the section *List of Deliverables* of the DoA.
- Deliverable Name is the official name of the deliverable as appearing in the section *List of Deliverables* of the DoA. The deliverable name is optional.
- vn.m is the document version, where n is the major version number and m is the minor version number (a.k.a revision Number). The version numbers are established by the responsible of the deliverable.

For example, the present document would be labeled as:

"SafeCloud-D7.2-Quality Assurance Plan-v1.0"

Deliverable internal reviews

If the internal review follows an in-line comment approach, such a review is recorded as indicated in the previous section.

Otherwise, in case of using a DRS, the code is defined as follows:

SafeCloud-Dx.y-Internal Deliverable Review Report-Partner

Where:

- Dx.y is the deliverable number under review, as reported in the cover page of the document. The resulting identifier must be one of that listed in the section *List of Deliverables* of the DoA.
- Partner is a compulsory field to identify the reviewer.

For example: "SafeCloud-D1.1-Internal Deliverable Review Report-UniNE"

Meeting minutes and documents

Meeting minutes are preferably on the SafeCloud wiki, sorted by date. Different types of meetings will be archives on different pages on the wiki. All documents relevant for a meeting, if any, are stored in a single meeting folder in the project git repository.

Internal WP reports

For WP intermediate reporting documents, the code is defined as follows:

`WPx_Internal Activity Report_Mzz_Vn.m`

Where:

- WPx is the identifier of the work package.
- Mzz is the month of reporting.
- Vn.m is the document version, where n is the major version number and m is the minor version number (a.k.a revision number). The version numbers are established by the responsible of the document.

Similarly, for partners intermediate reporting documents, the code is defined as follows:

`Partner_Internal WP Report_Mzz_Vn.m`

Where:

- Partner is the short name of a partner, as appearing in the DoA.

Logos

Project documents can be identified by adding the official logos:

Figure 1: SafeCloud logo 1

Figure 2: SafeCloud logo 2

Figure 3: SafeCloud logo 3

Other Conventions

In case of doubt the handbook for authors and translators in the European Commission [EUR14] will be used as a reference.

3.7.3 Documents versions

The version of a document appears in the name of said document. New versions of a document should include a "Version History" section to reflect a clear indication of what has been added, modified or removed with regard to the previous version. Comments or contributions on a document (e.g. in internal reviews) do not change the version. In MS Word documents the "Track Changes" function will be enabled and used.

3.7.4 Classification and storage

All relevant documents must be uploaded to the project repository and classified according to the defined folder structure. When not explicitly specified, the documents naming will include a representative name of the content, the partner responsible name and the date of the document.

It is advisable not to circulate the documentation through the distribution lists due to the size constraints in messages. Instead the link or path to the document in the repository can be included in the e-mail body.

Official public deliverables (those whose nature is labeled as "PU" in the list of deliverables in Annex I) will be also available at the project website (http://www.SafeCloud-project.eu) in PDF format.

3.8 Risk management

3.8.1 Risk dimensions

Similarly to any other project, SafeCloud will face certain situations that can affect its normal progress or even put it in danger. Predicting and anticipating these risky situations will provide the consortium with information to take decisions accordingly and act in time to minimise the impact. Therefore the risk management process is vital.

Risk management is a continuous process that can be represented by the cycle below. This cycle consists of four phases or levels: Identification of the risk, analysis and evaluation of the risk (probability and impact), response to the risk (risk avoidance, transfer, mitigation or acceptance) and monitoring of the success of contingency actions.

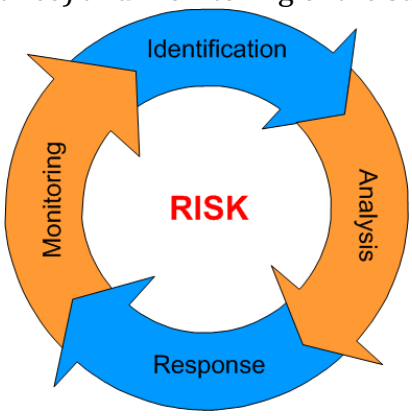

Figure 4: Risk cycle

Risk management should identify and alert from any deviation in the achievement of objectives (especially those included in the DoA) of any work plan (especially the DoA in all), in the foreseen timing (according to the Gantt chart, delivery dates and milestones), with the allocated resources (money and human) and with the expected quality.

3.8.2 Risk management tools

Regular meetings, communications and internal WP reports (at task level) help to identify potential risks in terms of timing and work progress. Quality assurance is guaranteed not only by the experience and knowledge of the involved individuals, but also because of the iterative delivery process for the delivery. Resources deviations will be tackled by means of the internal WP reports provided by each partner to the PC.

In addition to the project monitoring tools (internal WP reports) a risk register file will maintain record of the risks and their status at high level.
Regarding the specific case of software components, not only periodic meetings allow for risk reports but the partners also have access to common git repositories where software components and correspondent tests are available. These allow for partners to identify potential problems in software components and report them to the responsible partner. A problem report will describe the scenario where the problem was found and instructions on how to reproduce it. This allows the responsible partner to address the problem and manage the related risks.

3.8.3 Risk responsibility

All partners must be involved in the risk management process at the identification level and will inform about any risk that they can detect during the project execution. Any identified risk should be reported without delay to the person in charge.

Risks are handled by exception. In case a Task Leader is not able to manage a certain risk at task level, this risk will be raised to the Work Package Leader. Likewise, if a WPL is not able to manage a certain risk at WP level, the risk will be raised to the Scientific & Technical Committee or to the Project Management Board. Finally the risk will be raised to the EB.

3.8.4 Potential risks and correspondent contingency plan

Risk	Mitigation
Requirements for the use cases do not match the developed software components.	There is constant communication between the developers involved in the different WP software development. The use case requirements were detailed in specific deliverables that serve as reference for the development of SafeCloud software. Common software repositories are used to minimize future integration issues.
API incompatibilities in SafeCloud core components (WP1, WP2 and	Project management to ensure proper and early communications between WP and task leaders. Early release of API definitions such that other WP can build upon solid grounds and established functionalities definitions. Unit testing provided by component developers and integration testing.

WP3).	
Partners use more resources than planned.	Resource usage from the first year point to minimal risk of using more resources than planned. Nevertheless, good project management activities shall continue in the remaining time of the project.
Delays from one partner for contributing committed results.	Monthly call and face to face meetings minimize this risk. In the first year of the project partners have coordinated successfully for writing deliverables and preparing software integration.
Partner does not contribute sufficiently.	Project management to setup regular conference calls and meetings.
Significant delays in progress of the WP1-3, which are needed for WP4 and WP5.	Close interactions between work packages facilitated by key partners of work packages WP1-3 and monitored by the project management.
Deliverables or produced software do not meet sufficient quality standards.	Project management to establish quality assurance process, by systematically reviewing deliverables internally sufficiently ahead in time to allow corrections or additional work to be performed. Extensive software testing and cross-partner validation of requirements, APIs and performance.
Technical challenges prevent developed software to match promised solutions for each WP.	Solution design and architecture are strongly based on extensive study of related work and early stage prototypes. Continuous communication between partners allows to timely identify potential problems and challenges in order to address them adequately.

4 Standards and tools

4.1 Collaborative tools

4.1.1 Document sharing

All project-related documentation (organizational, legal, technical, financial) will be stored in the open source GIT distributed version control system (GIT). Each participant in the project has the right to have an account in this repository for content sharing purposes. Access control is the responsibility of UNINE and any request for access is addressed to that partner.

The root of the private area structure is split into WP folders. Inside each WP folder, there must be one folder for WP meetings documentation, with subfolders for each meeting. There must also be one folder for each task of the activity, and one subfolder per deliverable. Other required folders are possible, always with a descriptive name of the content. Each Work Package Leader is responsible for the organization and update of its WP folder.

Documents must be uploaded under their corresponding folder and named in a clear way for all users to have an idea of their content.

For prototype development, a dedicated GIT repository is also available. Developers should have access to this site. The request for access is addressed to the GIT server administrator (GIT), which is also UniNE.

4.2 Project templates

Project documents will be based on templates to ensure consistency throughout the project. Templates for presentations, deliverables, and meetings are available in the project repository. Each template contains the basic structure and format to develop the document. Other templates might be developed upon request.

4.3 Communication tools

4.3.1 Distribution lists

A set of email lists were set up at the beginning of the project to manage the information within each activity:

Mailing list	Scope	Address
Management	Distribution list for administrative and legal issues.	SafeCloud-mgmt@cs-lists.unine.ch
Technical	Technical and WP discussion.	SafeCloud-tech@cs-lists.unine.ch

Table 1: email lists

All lists are moderated by the Scientific & Technical Director. All partners are responsible to notify the STD for registration of new members and cancellations from the lists.

Email exchange between individuals aside from the lists is possible, but relevant threads must be kept within the distribution lists.

It is highly advisable to give a clear subject. This helps the creation of email rules to sieve the project emails from others in the inbox.

```
SafeCloud: WPx_Subject of the email
```

For example: “SafeCloud: WP1_Next meeting”.

4.3.2 Teleconference systems

Technical teleconference meetings are managed by UniNE and organized using the Vidyo conferencing system.

4.3.3 Website

The project website is another communication tool from the consortium to the target users (users groups, advisory board, and public at large). It aims at presenting the project framework, motivation and objectives, as well as promoting the project progress, events (also project-related events) and results (public deliverables).
The project website is accessible through the following URL: http://SafeCloud-project.eu/

UniNE is in charge of populating, maintaining and updating the information within the website. All partners must support UniNE by providing content of interest for the target users.

4.3.4 Post mail

Post Mails are necessary for formal communication related to official letters or documents among consortium members or between the PC and the EC.

5 References

[Eur14] European Commission. Directorate-General for Translation (2014), English Style Guide. A handbook for authors and translators in the European Commission, http://ec.europa.eu/translation/writing/style_guides/english/style_guide_en.pdf

[Eur15] European Commission (2015), Annotated Model Grant Agreement, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf

[Int14] International Organization for Standardization (2014), ISO 9000 essentials, http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/quality_management/iso_9000_essentials.htm

[Pat98] Patashnik O. (1998), BibTExting. http://ftp.gui.uva.es/sites/ctan.org/biblio/bibtex/contrib/doc/btxdoc.pdf